

## BICE Application Worksheets Glossary

Acceptance testing - testing to determine whether products meet the requirements specified in the contract or by the user

Access rights/privileges - privileges that are granted to a user, or perhaps to a program, to read, write and erase files in a computer system

Application - a computer program or set of programs that perform the processing of records for a specific business function/tasks, such as payroll, accounts payable, or inventory application

Application access - a granted privilege to use the application in some manner

Application access controls - internal controls over application access

Application code - programming language instructions produced by a compilation of a program

Application controls - programmed procedures in application software and related manual procedures, designed to help ensure completeness and accuracy of information processing (examples include computerized edit checks of input data, numerical sequence checks, and manual procedures to follow-up on items listed in exception reports)

Application environment - the environment in which the application resides, including everything that supports a system or the performance of a function and the conditions that affect the performance of a system or function

Application owner - the authority, individual, or organization who has original responsibility for the application by statute, executive order, or directive, responsibility which includes the policy and practice decisions of the application

Application (specific) controls – internal controls designed for an individual computer application, in contrast to controls related to IT infrastructure (i.e. general controls), that are directly related to individual computerized applications and help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported and which may include (1) programmed control techniques, such as automated edits (for example, edits designed to preclude users from entering unreasonably large dollar amounts in a payment processing system) and (2) manual follow-up of computer-generated reports, such as reviews of reports identifying rejected or unusual items

Application support - support provided by a professional with the appropriate technical skills and familiarity with the application

Assurance review - an objective examination of evidence for the purpose of providing an independent assessment on the efficiency and effectiveness of operations, compliance with laws and regulations, and accuracy and reliability of information

Audit charter – a document that formally defines and approves the purpose, authority, and responsibility of internal audit activity

Audit conclusion - professional judgment or opinion expressed by an auditor about the subject matter of the audit, based on and limited to reasoning the auditor has applied to audit findings

Audit finding - result of the evaluation of the collected audit evidence compared against the agreed audit criteria, which provides the basis for the audit report

Audit recommendation - part of the communicated results of an audit engagement, designed to enhance the internal control structure of the audited entity

**Audit trail** - a record of transactions in an information system that provides verification of the activity of the system; data in the form of a logical path linking a sequence of events, used to trace the transactions that have affected the contents of a record; a chronological record of system activities that is sufficient to enable the reconstruction, reviews, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results; a record showing who has accessed a computer system and what operations he or she has performed during a given period of time, useful both for maintaining security and for recovering lost transactions

**Auditee** - entity to be audited

**Auditing standards** - professional pronouncements promulgated by a recognized standards board that delineate the requirements for performing a broad range of audit activities and for evaluating audit performance

**Authentication** - proving the claimed identity of an individual user, machine, software component, or any other entity. Typical authentication mechanisms include conventional password schemes, one-time passwords, biometrics devices, and cryptographic methods.

**Authentication** – verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message; establishing the validity of a claimed identity, usually with a password

**Authorization** - the right or permission to use a system resource

**Automated control** - internal controls performed by computer, as opposed to manual controls

**Backup** - equipment or procedures available for use in the event of failure or overloading of regularly used equipment or procedures; a spare copy of a file, file system, or other resource for use in the event of failure or loss of the original

**Batch input** - the submission of batches of data through an input unit that has access to a computer through a data link

**Batch processing** – a method in which items are collected into groups or batches to permit convenient and efficient processing

**Business continuity plan** - see Disaster recovery plan

**Business process owner** - the user area with responsibility for the data/process, as opposed to the systems development area

**Business resumption plan** – see Disaster recovery plan

**Certify** – the validation by a qualified person guaranteeing the meeting of a certain standard

**Change procedures** - the processes to be used for all changes that are made to the computerized system and/or the system's data

**Compensating controls** – internal controls that reduce the risk of an existing or potential control weakness resulting in errors and omissions

**Control** – any protective action, device, procedure, technique, or other measure that reduces exposures

**Control totals** – accumulations of numeric data fields that are used to check the accuracy of input, processing, or output data

**Conversion** – the process of replacing a computer system with a new one

Critical (applications, data elements, data files, system files) - essential for continued operations

Critical success factor - a measure of success or maturity of a project or process that can be a state, a deliverable or a milestone

Cryptographic – of or pertaining to the various means and methods of rendering plain text unintelligible and reconverting cipher text into intelligible form

Data - distinct pieces of information, usually formatted in a special way, which can exist in a variety of forms; all software is divided into two general categories: data and programs

Data integrity - the state that exists when automated information or data is the same as that in the source documents and has not been exposed to accidental or malicious modification, alteration, or destruction

Data owner - the individual responsible for the policy and practice decisions of data

Disaster recovery plan – a plan that describes what steps and actions will be taken in the event of a disaster in order to make the continuation of normal functions possible, that consists of the precautions taken so that the effects of a disaster will be minimized and the organization will be able to either maintain or quickly resume mission-critical functions, and may also include a significant focus on disaster prevention

Edit routines - routines used to verify the accuracy or reasonableness of data or to modify the form or format of data, which may involve rearranging, adding (inserting dollar signs and decimal points) and deleting (suppressing leading zeros) data.

Encryption – the use of algorithms to encode data in order to render a message or other file readable only for the intended recipient; the process of scrambling data by a device or encoding principle (mathematical algorithms) so that the data cannot be read without the proper codes for unscrambling the data

End-user - a person who uses a computer application, as opposed to those who developed or support it, who may or may not know anything about computers, how they work, or what to do if something goes wrong and who doesn't usually have administrative responsibilities or privileges

General controls – General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect computer application programs, prevent system software from unauthorized access, and ensure continued computer operations in case of unexpected interruptions. General control areas typically include program change controls, telecommunications, LANs, WANs, servers, data centers, etc.

HIPAA – the acronym for the Health Insurance Portability and Accountability Act (of 1986) which requires the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers and also addresses the security and privacy of health data

Hash totals – summation for checking purposes of one or more corresponding fields of a file that would ordinarily not be summed

Implementation – the specific activities within the systems development life cycle through which the software portion of the system is developed, coded, debugged, tested, and integrated with existing or new penetration

Input controls – techniques and methods for verifying, validating, and editing data to ensure that only correct data enters a system

Interactive screen - computer screen allowing interactive participation by the viewer

Logical access - a user's view of the way security access is organized, the opposite of which is physical access/security

Offsite facility - a computer processing or storage area that is located away from the generating site

Operational testing - testing conducted to evaluate a system or component in its operational environment

Output controls - techniques and methods for verifying that the results of processing conform to expectations and are communicated only to authorized users

Manual controls - controls performed manually, rather than by computer

Material condition - a serious reportable condition in which the design or operation of the department's internal control structure does not adequately reduce, to an acceptable level, the risk that errors and irregularities can occur. Also, it is unlikely that the error or irregularity will be detected by management in a timely manner.

Migration - the process of moving from the use of one computing environment to another that is, in most cases, thought to be a better one

Performance indicator - a measure that shows the degree to which key processes achieve a desired level of performance. Performance indicators convey judgments about the adequacy of objectives or the quality of processes. Performance indicator systems monitor progress in achieving program goals and contribute to improvements by assessing implementation in terms of achieving desired objectives of the critical program processes.

Post-implementation review - an evaluation tool that compares the conditions prior to the implementation of a project (as identified in the business case) with the actual results achieved by the project

Processing controls - techniques and methods used to ensure that processing produces correct results

Production - the system environment in which an organization's data processing is accomplished versus the development environment or testing environment.

Real time processing - computer processing that generates output fast enough to support multiple activities being performed concurrently

Reconciliation - the process of balancing or getting two things to correspond, such as a checkbook and a bank statement

Reliability - the ability of a system or component to perform its required functions under stated conditions for a specified period of time

Reportable condition – a matter coming to management's attention that in their judgment should be internally communicated because it represents either an opportunity for improvement or an efficiency in management's ability to operate a program, or administer a process, effectively and efficiently

Residual risk - the remaining risk after risk management techniques have been applied

Restore – to retrieve a file from backup, if it has been accidentally erased or corrupted it can be restored if there is a backup.

Risk - a measure of uncertainty that may involve negative consequences

Risk analysis - the assessment, management and communication of risk

Risk assessment - the identification of risk, the measurement of risk, and the process of prioritizing risks

Risk-mitigating - elimination or reduction of risk exposure

Run-to-run totals - before and after file comparisons

SAS 70 - SAS (Statement on Auditing Standards) No. 70 is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants. SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion is issued to the service organization at the conclusion of a SAS 70 examination.

Safeguard – precautionary measure warding off impending danger, damage, injury, etc.

Self-assessment – an assessment performed by the responsible organization to determine how well it is performing and meeting its responsibilities

Sensitive data files - data files that require protection and that should not be made generally available

Segregation/separation of duties - assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets, in order to reduce the opportunities for one person to both perpetrate and conceal errors or fraud

Source documents - the paper form onto which data are written (examples are order forms and employment applications)

Stakeholder - an individual or group with an interest in the success of an organization in delivering intended results and maintaining the viability of the organization's products and services. Stakeholders influence programs, products, and services.

Suspense file - entry of disallowed information may cause a transaction to be posted to a suspense file, denoting that further attention or action is required

System - a group of related components that interact to perform a task; may consist of infrastructure (physical and hardware components), software, people, manual and automated procedures, and data

System development life cycle – the sequence of events in the development of a system

Terminal device number – identification number of a computer terminal

Trusted path - a path for accessing permitted actions and commands, with all elements writeable only by trusted users and which cannot be imitated by untrusted software

Validation control - a process used to detect or prevent data that is inaccurate, incomplete, unreasonable, incorrect or noncompliant with applicable standards, rules, and conventions